Combinatorial Designs and Groups*

by Marshall Hall, Jr.
California Institute of Technology

1. Introduction. Construction of designs by assuming a certain automorphism group is a powerful method first developed extensively by R. C. Bose. Recently the symmetric designs with $v = 56$, $k = 11$, $\lambda = 2$ and $v = 79$, $k = 13$, $\lambda = 2$ have been constructed by such methods. Examples of this method, including these two are given in section 2.

Section 3 studies groups generated by a class C of elements of order 3 in which any two non-commuting elements generate SL(2,3). Here the four groups of order 3 in SL(2,3) may be considered a block of 4 points, and the study of such groups may be related to designs with $k = 4$, $\lambda = 1$.

2. Applications of groups to combinatorial designs. If designs with given parameters exist then usually there is such a design with a non-trivial group of automorphisms. Assuming the existence of a group of automorphisms may be of great help in the construction of the design, and also simplify the presentation of the design. The simplest case is that in which a design with v elements has a cyclic group of automorphisms of order v which permutes the elements cyclically. In such a case we may identify the elements with the residues modulo v, and let $\alpha : i \to i + 1 \pmod v$ be a generator of the automorphism group. The symmetric block design with $v = b = 73$, $r = k = 9$, and $\lambda = 1$ is such a design. Here the elements of one block B_1 may be taken as the set

2.1) $B = \{1,2,4,8,16,32,37,55,64\} \pmod{73}$

* This research was supported in part by ONR Contract N00014-67-A0094-0010

and the mapping $i \to i + 1 \pmod{73}$ maps B_1 into all 73 blocks. This design is the projective plane of order 8. The fact that the residues in 2.1) do form a block of such a symmetric design is equivalent to showing that every residue $d \not\equiv 0 \pmod{73}$ is the difference $a_i - a_j$ of two residues a_i, a_j in 2.1) in exactly $\lambda = 1$ ways. Thus we refer to the set B in 2.1) as a difference set. In this example the design also has the further automorphism $u : i \to 2i \pmod{73}$ and we say that 2 is a multiplier of the difference set design. It has been proved [8] that a difference set $a_1, \ldots, a_k \pmod{v}$ determining a design with parameters $b = v$, $r = k$, and λ has a multiplier p where p is a prime such that (i) $(p,v) = 1$, (ii) $p \mid k - \lambda$ and (iii) $p > \lambda$. In all known examples condition (iii) is unnecessary, but no proof has been found which does not use some variant of it. Elimination of condition (iii) is a challenging, but difficult problem.

The example given in 2.1) has a further interesting property. The residues listed are the octic residues of the prime $p = 73$. This relates difference sets to the problems of cyclotomy, and new classes of designs based on this approach have been found by Whiteman [10] and others. It has been noted by the writer [5] that determining cyclotomic constants is equivalent to the calculation of certain group characters.

The 36 points (x,y) where x and y range independently over the residues modulo 6 under addition form a group G of order 36. The 15 points

2.2)
$$\begin{array}{c} (1,1),(2,2),(3,3),(4,4),(5,5) \\ (0,1),(0,2),(0,3),(0,4),(0,5) \\ (1,0),(2,0),(3,0),(4,0),(5,0) \end{array}$$

if taken as a block B_1, together with its images under the action of G form a symmetric design with $v = b = 36$, $r = k = 15$, $\lambda = 6$.

There may be several orbits of points and also several orbits of blocks under the action of the group. This is the essence of R. C. Bose's "method of symmetrically mixed differences" [2]. For example with G the additive group of residues modulo 5, we may take three orbits of length 5 distinguishing the orbits by subscripts, having points i_1, i_2, i_3 with i modulo 5 to give $v = 15$ points. To obtain the Steiner triple system with $v = 15$, $b = 35$, $r = 7$, $k = 3$, $\lambda = 1$, the blocks fall into 7 orbits and representatives of these block orbits form "base blocks" which determine the rest: A set of base blocks is

$$2.3) \qquad \begin{aligned} &(0_1,1_2,4_2),(0_1,2_2,3_2),(0_2,1_3,4_3),(0_2,2_3,3_3),\\ &(0_3,1_1,4_1),(0_3,2_1,3_1),(0_1,0_2,0_3). \end{aligned}$$

More recently the relationship between permutation groups and block designs has been studied [6]. If D is a design which has an automorphism group G transitive on the points of D and also on the blocks of G, then if we represent G as a permutation group on the points, then if H is the stabilizer of a block B_1, clearly B_1 consists of complete orbits of H. If H is also the stabilizer of a point we call D an orbital design. Any transitive permutation group will yield orbital designs which are partially balanced block designs in the sense of Bose and Shimamoto [3]. A case of particular interest is the study of rank 3 groups. The theory of these groups has been developed by D. G. Higman [9].

The group $G = PSL_3(4)$ is the little projective group of the plane π of order 4, which contains 21 points. An oval in π is a set of 6 points

no three on a line, and an oval is determined by any 4 of these. The plane π contains 168 ovals which are permuted by G in three orbits of 56 ovals. Representing G as a permutation group on one set of 56 ovals, G is generated by the permutations

2.4)
$$\begin{aligned} a &= (1,2,3,4,5,6,7)(8,9,10,11,12,13,14)(15,16,17,18,19,20,21)\\ &\quad (22,23,24,25,26,27,28)(29,30,31,32,33,34,35)\\ &\quad (36,37,38,39,40,41,42)(43,44,45,46,47,48,49)\\ &\quad (50,51,52,53,54,55,56)\\ c &= (1)(2,8,41)(3,27,28)(4,35,31)(5,20,53)(6,14,22)(7,42,54)\\ &\quad (9,29,34)(10,52,17)(11,24,46)(12,30,48)(13,55,33)\\ &\quad (15,26,32)(16,21,56)(18,40,35)(19,23,49)(25,50,44)\\ &\quad (37,51,47)(38,39,43)(45) \end{aligned}$$

G is a rank 3 group in which a stabilizer has orbits of lengths 1,10,45. The letter 1 and the orbit of length 10 in G_1 are

2.5) $$B = \{1,12,19,23,30,37,45,47,48,49,51\}.$$

The set $B = B_1$ and its images under G form a symmetric block design with $v = 56$, $k = 11$, $\lambda = 2$. This construction [7] was the first for this design.

A symmetric block design with $v = 79$, $k = 13$, $\lambda = 2$ was constructed by Aschbacher [1] with an automorphism group G which is the Frobenius group of order 110. We define G by

2.6) $$G = \langle x,y,z \mid x^{11}=y^5=z^2=1,\ y^{-1}xy = x^4,\ z^{-1}xz = x^{-1},\ yz = zy\rangle.$$

We take B_1,B_2,B_3,B_4 as base blocks and P_1,P_2,P_3,P_4 as base points. Let H_i be the stabilizer of P_i and G_j be the stabilizer of B_j. These are

defined by

2.7) $$H_1 = \langle x,y\rangle,\ H_2 = H_3 = \langle y,z\rangle,\ H_4 = \langle z\rangle$$
$$G_1 = G_2 = G,\ G_3 = \langle y\rangle,\ G_4 = \langle z\rangle.$$

Incidence on the base blocks is defined by

2.8)
$$B_1 : \{P_1, P_1z, P_2G\}$$
$$B_2 : \{P_1, P_1z, P_3G\}$$
$$B_3 : \{P_1, P_2, P_3, P_4xy^i, P_4x^4y^j\}$$
$$B_4 : \{P_2x^{\pm 2}, P_3x^{\pm 5}, P_4, P_4x^{\pm 1}y^2, P_4x^{\pm 1}y, P_4x^{\pm 5}y, P_4x^{\pm 5}y^4\}.$$

3. An application of the theory of designs to groups. The Conway group [4] contains a class of elements of order 3 such that any two which do not permute generate SL(2,3) of order 24, SL(2,5) of order 120 or their factor groups by a center of order 2 which are respectively A_4 and A_5. It is therefore of interest to determine those groups generated by such a class of elements of order 3. Here the more restricted case is examined in which there is a class of elements of order 3 in which any two elements either commute or generate SL(2,3) or its factor group A_4.

Defining relations for SL(2,3) are

3.1) $$a^3 = b^3 = abab^{-1}a^{-1}b^{-1} = 1.$$

We write $a \sim b$ as an abbreviation for these relations. We note that if $a \sim b$ then $a^{-1}ba = bab^{-1}$ so that a and b are conjugate. But we do not have $a^{-1} \sim b$, though we do have $a^{-1} \sim b^{-1}$. Thus in 3.1) there is a distinction between the generators a and a^{-1}, b and b^{-1} of the groups $\langle a\rangle$ and $\langle b\rangle$ of order 3.

Taking groups of order 3 such as $\langle a \rangle$ generated by an element a of our class C as points, then we associate with $SL(2,3) = \langle a,b \rangle$ where $a \sim b$ a block of 4 points, namely $\langle a \rangle$, $\langle b \rangle$, $\langle a^{-1}ba \rangle$, $\langle b^{-1}ab \rangle$, these being the 4 conjugate subgroups of $SL(2,3)$ and we note that $x \sim y$ where x and y are any two of $a, b, a^{-1}ba, b^{-1}ab$. Thus we have a block of size $k = 4$ and $\lambda = 1$ as any two distinct points determine the block.

For three elements a,b,c of the class C in which $a \sim b$, the possibilities for $G = \langle a,b,c \rangle$ are

1. $ca = ac$, $cb = bc$. Here $\langle a,b,c \rangle = \langle a,b \rangle \times \langle c \rangle$.

2. $ca = ac$, $c \sim b$. Here $|G| = 648$

and putting $h = a^{-1}c$, G has a normal subgroup $H = \langle h, b^{-1}hb \rangle$ of exponent 3 and order 27 and $G/H = \langle a,b \rangle$.

3. $c \sim a$, $c \sim b$, $c \sim a^{-1}ba$, $c \sim b^{-1}ab$.

Here $|G| = 768 = 2^8 \cdot 3$. G has 16 subgroups conjugate to $\langle a \rangle$, and the center of G contains $(a^{-1}b)^2$, $(a^{-1}c)^2$, and $(b^{-1}c)^2$.

4. $c \sim a$, $c \sim b$, $c \sim a^{-1}ba$, $c^{-1} \sim b^{-1}ab$.

These relations make G collapse so that $G = 1$.

5. $c \sim a$, $c \sim b$, $c^{-1} \sim a^{-1}ba$, $c^{-1} \sim b^{-1}ab$.

Here $|G| = 6048$ and G has 28 groups conjugate to $\langle a \rangle$.

In case 3 the 16 conjugates of $\langle a \rangle$ form the block design with $v = 16$, $b = 20$, $r = 5$, $k = 4$, $\lambda = 1$, the affine plane of order 4. In case 5 the 28 conjugates of $\langle a \rangle$ form a block design D with $v = 28$, $b = 63$, $r = 9$, $k = 4$, $\lambda = 1$. Here $G = U_3(3)$ the 3 dimensional unitary group over $GF(3^2)$. The points may be identified with the 28 isotropic points in the projective plane over $GF(3^2)$, and these lie in sets of 4 on 63 lines.

With 3 or more generators from C, unless case 5 arises, the elements of C are not conjugate to their inverses and G has a normal subgroup of index 3. We consider $G = \langle a,b,c,d \rangle$ where $\langle a,b,c \rangle = U_3(3)$ as in case 5 and d is a further element of C. If $\langle r \rangle, \langle s \rangle, \langle t \rangle, \langle u \rangle$ are one of the 63 blocks and r,s,t,u are conjugate in $\langle r,s \rangle$, then if d does not permute with any one of these, we have $\langle d,r,s \rangle$ a group of type 3 or type 5 above. Take $x_1 = a$, $x_2,\ldots,x_{28}$ as generators of the 28 groups conjugate to $\langle a \rangle$ in $U_3(3)$ and choose the generator x_i of $\langle x_i \rangle$ so that $x_i \sim a$ rather then $x_i^{-1} \sim a$. Then one of the 63 blocks r,s,t,u will consist of four of $x_1 \ldots x_{28}$ and their inverses. If d does not permute with any one of r,s,t,u, then in case 3 we have $d \sim r$, $d \sim s$, $d \sim t$, $d \sim u$ or $d^{-1} \sim r$, $d^{-1} \sim s$, $d^{-1} \sim t$, $d^{-1} \sim u$, and in case 5, $d \sim r$, $d \sim s$, $d^{-1} \sim t$, $d^{-1} \sim u$ or some other combination involving d twice and d^{-1} twice. If we have say d three times and d^{-1} once we are in case 4 and the group collapses. If d permutes with exactly one of r,s,t,u, say $dr = rd$, then we are in case 2 and $d \sim s$, $d \sim t$, $d \sim u$ or $d^{-1} \sim s$, $d^{-1} \sim t$, $d^{-1} \sim u$. Hence we must for each of $x_1,\ldots,x_{28}$, say that $dx_i = x_i d$, or $d \sim x_i$ or $d^{-1} \sim x_i$ so that with d and any one of the 63 blocks r,s,t,u we avoid case 4. This turns out to be a strong restriction. We summarize the results:

First case: d permutes with no one of $x_1,\ldots,x_{28}$. Two essentially different patterns arise. First d may mimic the relation of some x_i to the rest. By conjugation we may take this to be $x_1 = a$ and then $d \sim x_i$, all i. Here $d \sim x_i$, $i = 1, \ldots 28$. But then from case 3 for d with r,s,t,u, we have $(r^{-1}s)^2 d = d(r^{-1}s)^2$. There are enough of these $(r^{-1}s)^2$ so that $\langle (r^{-1}s)^2 \ldots \rangle$ contains a and we conclude $da = ad$ contrary to assumption. In a second pattern the group $\langle a,c,d \rangle$ is in case 3 and also $\langle (r^{-1}s)^2 \cdots \rangle$ centralizing d contains aca. But daca = acad together with $\langle a,c,d \rangle$ in case 3 collapses to $a = c = d = 1$.

Hence no group arises in this first case.

Second case: d permutes with exactly one of $x_1,\ldots,x_{28}$ which we take to be $x_1 = a$. The only permissible pattern is $d \sim x_i$, $i = 2,\ldots 28$. Here putting $d = a$ maps G homomorphically onto $U_3(3)$. The kernel is generated by conjugates of $h = a^{-1}d$. From computer studies by J. Cannon, the kernel presumably a 3 group, is of order at least 3^{10}.

Third case: d permutes with exactly two generators of $x_1,\ldots,x_{28}$, say $da = ad$, $db = bd$. Then G is of order 117,573,120, as calculated by J. Cannon. This must have $U_4(3)$ as a factor group, and has a normal subgroup of order 36 which will be central.

Of course a fourth case is that in which d permutes with all of $x_1,\ldots,x_{28}$ and here $G = \langle d \rangle \times U_3(3)$.

References

[1] M. Aschbacher "Collineation groups of symmetric block designs" to appear in J. Comb. Theory.

[2] R. C. Bose "On the construction of balanced incomplete block designs" Ann. Eugenics 9(1939), 353-399.

[3] R. C. Bose and T. Shimamoto "Classification and analysis of partially balanced incomplete block designs with two associate classes" J. Amer. Stat. Assn. 47(1952), 151-184.

[4] J. H. Conway "A group of order 8,315,553,613,086,720,000" Bull. London Math. Soc. 1(1969) 79-88.

[5] Marshall Hall, Jr. "Characters and cyclotomy" Proc. Symposia in Pure Math. Amer. Math. Soc. 8(1965), 31-43.

[6] _____ "Designs with transitive automorphism groups" to appear.

[7] M. Hall, Jr., R. Lane, and D. Wales "Designs derived from permutation groups" J. Comb. Theory 8(1970) 12-22.

[8] M. Hall, Jr. and H. J. Ryser "Cyclic incidence matrices" Can. J. Math 3(1951), 495-502.

[9] D. G. Higman "Finite permutation groups of rank 3" Math. Z. 86(1964) 145-156.

[10] A. L. Whiteman "A family of difference sets" Ill. J. Math. 6(1962) 107-121.